Securing Our Skies

Terrorist attacks involving aircraft continue to be of great interest to al Qaeda and a major threat to the security of the United States. Despite massive federal investments in aviation security since September 11, major security gaps remain. Serious deficiencies have been revealed in many of the "layers" of security the Transportation Security Administration has put in place at our nation's airports. To close security gaps in the aviation system, the Transportation Security Administration should improve the performance of its screening workforce, take aggressive steps to secure air cargo, adopt new measures to defend aircraft against missile attack, and improve controls over access to sensitive airport locations and airplanes.

The terrorist attacks of September 11 exploited several shortcomings in U.S. aviation security. The hijackers were not stopped from boarding aircraft by pre-screening systems or security inspections and were able to gain control of aircraft once airborne. The response to these heinous attacks was, in part, to create a new federal agency to ensure the security of passenger and cargo aircraft. Under demanding statutory deadlines, the Transportation Security Administration (TSA) hired an army of security screeners, reaching a one-time high of 54,600 personnel. Congress has provided TSA with a total of $10.7 billion for passenger and baggage screening.[1]

The threat of terrorist attacks on aircraft, or using aircraft as weapons, remains vivid. When raising the nation's threat level to "High" on December 21, 2003, Secretary Ridge stated that, "Recent reporting reiterates … that al-Qaida continues to consider using aircraft as a weapon. And they are constantly evaluating procedures both in the United States and elsewhere to find gaps in our security posture that could be exploited."[2]

Congressional mandates and TSA regulations have led to a number of additional steps over the past two years to improve aviation security. The number of air marshals riding on flights has increased from 33 on September 11 to thousands.[3] All U.S. passenger aircraft, as well as foreign flights arriving or departing in the United States, now have hardened cockpit doors. In its first year and a half of airport screening, more than 7.5 million prohibited items, including nearly 2.3 million knives, 1,437 firearms and 49,331 box cutters were taken from passengers.[4] Recently, several commercial flights were delayed, cancelled, or escorted by military aircraft when deemed to be at significant risk of a terrorist attack. Finally, TSA has rightly emphasized a "layers of defense" strategy, employing multiple protective measures to guard against terrorist attack.

---

[1] Appropriation levels from Public Laws 107-87, 107-117, 108-7, 108-11, 108-90, and 108-206. The figure includes fees levied on passenger tickets.

[2] See U.S. Department of Homeland Security Press Office, "Threat Level Raised, Remarks by Secretary of Homeland Security Tom Ridge," December 21, 2003. http://www.whitehouse.gov/news/releases/2003/12/20031221.html.

[3] The exact number of federal air marshals (FAMs) is classified, but is in the few thousands. On November 25, 2003, the FAM program was moved from TSA to the DHS Bureau of Immigration and Customs Enforcement.

[4] Transportation Security Administration, "State of Aviation Security Fact Sheet," September 29, 2003. http://www.tsa.gov/public/display?theme=8&content=0900051980057f92.

However, despite the progress and the vastly heightened public awareness to the threat of hijacking, major vulnerabilities remain in our aviation system. Several of the layers of defense have significant security gaps. The TSA must address ongoing problems with aviation security, including concerns about the efficacy of airport screening, the lack of security for air cargo, the potential threat from shoulder-fired missiles, and unauthorized access to aircraft or other secure airport areas.

SECURITY GAP: Passenger and Baggage Screening Allows Significant Numbers of Dangerous Items Aboard Aircraft.

The DHS Office of the Inspector General, the General Accounting Office (GAO), and the TSA's own investigation team have all conducted undercover investigations and found that prohibited items – including, according to media reports, firearms and simulated explosive devices – are still passing through TSA screening checkpoints. Comparisons with similar investigations conducted before TSA started its screening operations show that much improvement is still needed.[5] Security tests by media groups and private citizens have also demonstrated flaws in the security screening process.[6] Statements by TSA employees suggest that a number of checked bags are not even subjected to screening measures, in one case alleging that "federal baggage screeners run only a small portion of suitcases through explosives-detection devices."[7] Current screening systems are not capable of routinely catching passengers that have hidden explosives on themselves.

Appropriate screener staffing levels, better detection technology, and a stronger training program would greatly decrease these security shortfalls.

- **Screener Staffing**

Having the appropriate number of screeners at airport security checkpoints is critical to aviation security. Too few screeners leads to increased passenger wait times, which in turn applies pressure on TSA personnel to take security shortcuts. According to a recent GAO study, insufficient screener staffing has led to an inability to fully utilize detection equipment and to access all training programs.[8] These problems stem from an October, 2003 congressional decision to cap the TSA screener level at 45,000 due to concerns about escalating costs and a

---

[5] Specific results of screener testing are sensitive and not publicly released. Information obtained from General Accounting Office and Department of Homeland Security Office of Inspector General. Previous FAA studies uncovered a 20 percent failure rate to identify prohibited items, and failure rates increased when tests were made to more accurately predict how terrorists might try to conceal weapons (GAO, *Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations, GAO-01-1171T*, (Washington: U.S. General Accounting Office, September 25, 2001), 5-6.

[6] In one investigation since 9/11, it was reported that prohibited items cleared passenger security for all 14 flights attempted at 11 airports. Maki Becker and Greg Gittrich, "Weapons Still Fly at Airports: News Boards 14 Jets with Contraband Despite Security Push," *Daily News*, September 4, 2002, 7.

[7] Confidential interviews between TSA employees and staff of the House Select Committee on Homeland Security. See also Sharon Linstedt, "Ex-Chief Calls Gaps in Security 'Serious'," *The Buffalo News*, February 11, 2004, B1.

[8] GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening, GAO-04-440T*, (Washington: U.S. General Accounting Office, February 12, 2004), 3, 16.

growing screener workforce.[9] However, no comprehensive personnel study has been conducted to ensure that this personnel level is the number necessary to adequately screen all passengers and checked baggage. Nonetheless, TSA has sought to comply with this congressional mandate and has reset staffing levels at all airports. As of February 9, 2004, TSA screener staffing was below the overall national cap of 45,000.[10]

SECURITY RECOMMENDATION

The TSA, working with airport authorities, should conduct a comprehensive study to determine how many screeners are actually necessary to implement appropriate security procedures at all checkpoints. This study should include analysis of current passenger traffic, which varies regularly with flight schedules and seasonal demand, in order to provide the number of screeners required for full security. The TSA should recognize in this study that the presence of long passenger delays at security checkpoints is likely to place pressure on screeners to take shortcuts in security, and account for such a possibility accordingly. Congress should then revise the 45,000 screener cap imposed in 2003, if warranted, and it should provide TSA with the funding required to support a screener workforce that meets those demands.

- **Screening Technology**

The technology for both passenger and baggage screening deployed at U.S. airports is still substantially the same as what was in place before September 11[11] and TSA has not acted aggressively to develop and deploy new technology. In fact, in fiscal year 2003, TSA shifted $60 million out of $75 million appropriated for technology development to cover shortfalls in its current operating budget.

TSA and private companies have identified promising technologies that can better locate and identify concealed explosives and other dangerous items, which would greatly improve screeners' ability to prevent these items from getting onto aircraft. For example, technologies exist that can detect explosives residue on passengers, which cannot be identified with currently deployed detectors. This particular security gap was exposed when would-be terrorist Richard Reid was able to bring roughly ten ounces of explosives onto an American Airlines international flight, and he was only stopped from carrying out a terrorist attack by alert passengers. According to GAO, "TSA is funding [research and development] on several technologies designed to improve the screening of checked baggage and passengers at the nation's airports. However, while the majority of these technologies are scheduled for pilot testing within the next 12 to 18 months, they are not scheduled to be deployed in quantity for 2 to 5 years."[12]

---

[9] House Report 108-280 accompanying "Department of Homeland Security Appropriations Act of Fiscal Year 2004." (P.L. 108-90).

[10] Briefing from DHS Budget Office staff for Select Committee on Homeland Security staff, February 9, 2004.

[11] See testimony of Stephen McHale, Deputy Administrator, Transportation Security Administration. U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003. According to McHale, "I agree with you completely that the technology we're using is somewhat better than 9/11 but not a lot. It is the same type of technology."

[12] GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening, GAO-04-440T,* (Washington: U.S. General Accounting Office, February 12, 2004), 32.

Additionally, TSA has not adequately deployed technology that already exists. It has failed to install explosives detection technology needed to fully screen checked baggage at a number of airports, despite a legal requirement to do so this by December 31, 2003.[13] At least five airports are still reportedly using hand inspections, canine teams, and passenger-bag matching to secure baggage placed on commercial aircraft.[14] One reason that screening equipment has not been installed at all airports is that current detectors are too large to fit into many existing airport structures.[15] New technologies can provide smaller, but equally or more capable, screening equipment that would fit into existing infrastructure.

Another technology, the Threat Image Projection (TIP) System, is not being fully deployed at U.S. airports. The system tests screener performance by rating their ability to identify weapons that virtually are inserted by the detection equipment software into images of bags going through the screening process. The TIP system had been discontinued at passenger screening checkpoints after September 11[16] but has recently been restored. However, the system is not used in screening of checked baggage.[17]

SECURITY RECOMMENDATION

The TSA should invest more in developing, evaluating, and deploying screening technologies. Better technology will improve current screening performance and provide an ability to identify objects that are currently undetectable so as to decrease the likelihood of an armed hijacking or explosion aboard a passenger airplane, and minimize disruption at airports. TSA should increase the use of pilot programs and other means to rapidly deploy new technologies into airports.

- **Screener Training**

During the TSA's two years of operation, a number of problems relating to screener training have been revealed. The TSA addressed most of these issues once they were publicized, but it has not demonstrated a proactive approach to ensuring proper training among the screener or supervisory workforce.

All TSA screeners are required to undergo roughly 100 hours of training, consisting of classroom learning, written tests, and on-the-job skills training. Screeners are also subject to annual tests and are required to undergo immediate remedial training if they fail to demonstrate appropriate

---

[13] "Homeland Security Act of 2002" (P.L. 107-296, §425). The deadline was initially set for December 31, 2002 in the Aviation and Transportation Security Act, (P.L. 107-71 §110).

[14] The Homeland Security Act ("Homeland Security Act of 2002" (P.L. 107-296, §425)) requires the Administrator of the TSA to report to Congress on the airports that are not electronically screening 100 percent of checked baggage, but these reports are classified. See also (a) Congressional Research Service, *Aviation Security: Issues before Congress Since September 11, 2001. RL31969*, (Washington: Congressional Research Service, June 18, 2003), 5; (b) Jeffrey Leib, "DIA Likely To Miss Screening Deadline," *Denver Post*, December 16, 2003, B1; and (c) Ron Marsico, "Airport Still Fails to Meet Bomb Rules," *The Star-Ledger*, January 1, 2004, 13.

[15] GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs, GAO-04-285T*, (Washington: U.S. General Accounting Office, November 20, 2003).

[16] GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining, GAO-03-1173*, (Washington: U.S. General Accounting Office, September 24, 2003).

[17] GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening, GAO-04-440T*, (Washington: U.S. General Accounting Office, February 12, 2004), 21.

screening techniques. It is unclear to what extent this training is meaningful, and whether the testing is a good indication of screener proficiency. According to the DHS Office of Inspector General:

> "Newspaper articles reported that Transportation Security Administration (TSA) airport baggage screeners were given the answers to the questions prior to taking the final examination for certification.… TSA confirmed that 22 of the 25 questions on the final examination were the same as those used for daily lesson quizzes, concluded that the testing was conducted as prescribed by TSA, and found no misconduct on the part of the instructors…."When the OIG learned of TSA's conclusions, we initiated our own review. **We were disturbed to learn that the screeners had, in fact, been given the answers to the final examination beforehand and to learn that TSA saw nothing wrong with this.** Our review confirmed that many of the final examination questions were identical or similar to questions that were given to the examinees in practice examinations. Furthermore, we found that many of the answers to the questions were obvious. **Accordingly, there could be no assurance from the testing program that the examinees had been trained to identify explosive devices in checked baggage.** In response to the OIG report, TSA promises to revise its testing program. The OIG will monitor this and undertake a complete review of TSA's testing and training programs."[18] (emphasis added)

According to GAO, "TSA has deployed basic and remedial screener training programs, but has not fully developed or deployed a recurrent or supervisory training program to ensure that screeners are effectively trained and supervised."[19] Furthermore, supervisors that oversee screening operations have not necessarily undergone basic screening training themselves. As GAO notes, "TSA encourages, but does not require, screening managers, who are responsible for overseeing screening functions to participate in classroom training, even if they do not have prior screening experience."[20] The TSA has recently begun identifying appropriate training programs, but will not have a fully trained supervisory workforce at the nation's airports for several months at minimum.

By law,[21] five airports were designated by TSA to have non-federal screener workforces to serve as a basis for comparison after two years of TSA operations. Training at these non-TSA screener airports has been problematic. Under this program, airports and private screening services must meet the same overall hiring, training and security requirements as federal screeners.[22] However, the security directors at these airports have struggled to get training products from TSA, hindering security and making comparisons of security at these and other airports difficult. According to officials with McNeil Security, the company providing security for Rochester International Airport, "[i]t is a fact that while numerous wait time surveys have been conducted

---

[18] Department of Homeland Security Office of Inspector General. Semiannual Report to the Congress, April 1, 2003 – September 30, 2003, 5. http://www.dhs.gov/interweb/assetlibrary/OIG_Fall_2003_SAR.pdf.

[19] GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining, GAO-03-1173*, (Washington: U.S. General Accounting Office, September 24, 2003), 2.

[20] GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining, GAO-03-1173*, (Washington: U.S. General Accounting Office, September 24, 2003), 7.

[21] "Aviation and Transportation Security Act" (P.L. 107-71 §108).

[22] Testimony of John Demill, President, Firstline Transportation Security. U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003.

and there has been little or no recurrent training provided except which McNeil Security provided. Screening supervisors are giving no additional training beyond the basic screen training course …. It is not possible to identify those areas where screeners may need additional training. Screeners were supposed to be ranked by their test performance [during TSA inspections]. This is important information for corporate actual performance reviews. To date, this information has not been provided."[23]

SECURITY RECOMMENDATION

Taken together, these cases demonstrate, at best, a lack of attention to appropriate screener and supervisor training. The TSA should ensure that every screener and supervisor is subject to, and demonstrates mastery over, all TSA screening procedures. The TSA and DHS should conduct routine tests at multiple airports to ensure that training is conducted appropriately and that active screeners are applying the training adequately. All screeners and supervisors should have rigorous recurrent training on an annual basis that consists more than cursory tests of routine screening procedures.

SECURITY GAP: Unscreened Air Cargo on Passenger Aircraft and Air Cargo Flights Remains Vulnerable to Exploitation.

Air cargo – freight, packages, and mail carried aboard passenger or all-cargo aircraft – continues to be a major security shortcoming. Roughly 2.8 million tons of cargo is transported by passenger planes annually, constituting 22 percent of all air cargo.[24] Terrorists have previously exploited the lack of security in packages carried on planes: a device in a baggage container of Pan Am Flight 103 exploded on December 21, 1988, over Lockerbie, Scotland;[25] and the FBI determined that an explosion aboard a November 15, 1979, U.S. airliner was caused by a parcel shipped by U.S. mail as air cargo, linked to the "Unabomber" Theodore Kaczynski.[26] The TSA officials have determined that the risk of a terrorist bomb in air cargo has increased because the federal government is focused almost exclusively on screening passengers and luggage. According to a media characterization of a TSA report, "[c]argo is likely to become – and may already be – the primary threat vector in the short term." [27] There is a 35 percent to 65 percent likelihood that terrorists are planning to put a bomb in cargo on a passenger plane, another TSA document said, citing year-old intelligence reports.[28]

---

[23] U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003.
[24] GAO, Aviation *Security: Efforts to Measure Effectiveness and Strengthen Security Programs, GAO-04-285T*, (Washington: U.S. General Accounting Office, November 20, 2003), 20.
[25] See GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington: U.S. General Accounting Office, December 20, 2002), Appendix I: Air Cargo Incidents and Follow-Up Actions, 22.
[26] Affidavit of Assistant Special Agent in Charge, Terry D. Turchie, Before the U.S. District Court, District of Montana, April 3, 1996.
[27] Greg Schneider, "Terror Risk Cited For Cargo Carried On Passenger Jets; 2 Reports List Security Gaps," *Washington Post*, June 10, 2002, A1.
[28] Ibid.

The Administration requested no dedicated funds for air cargo in its the fiscal year 2004 budget, but Congress provided $85 million for this need. The Administration's fiscal year 2005 budget request does not include any increase over the $85 million level funded in 2004.[29]

Despite the clear threat and a legal mandate to provide for the screening of all cargo carried on passenger aircraft,[30] TSA instead relies on random inspections and a "known shipper program" that has been shown to have several security shortcomings.[31] No cargo can be placed aboard a passenger aircraft unless the sender is a participant in the "known shipper" program, and those shippers are required to follow a set of security practices prescribed by TSA. However, TSA does not verify compliance with security regulations for all "known shipper" companies.[32] In cases where verification is done, "TSA inspectors have found numerous security violations made by freight forwarders and air carriers during routine inspections of their facilities."[33] Further, "Employees of shippers and freight forwarders are not universally subject to a background check.[34] Moreover, no air cargo, including U.S. mail, weighing less than 16 ounces is screened or subject to any other security measures.[35] Former TSA Administrator and current DHS Deputy Secretary, Admiral James Loy, testified in 2002 that "it is absolutely an imperative that we spend focused attention on getting a better approach to cargo. We have strengthened the known shipper program from what it used to be, but I do believe that it's still simply not enough …. [W]e must reach to [secure] cargo better."[36]

Department of Homeland Security officials have stated that, "Analysis performed by Battelle Corporation on behalf of FAA in 2001 determined that only a small percentage of the nation's air cargo could be physically screened efficiently with the available technology without significantly impending the supply chain. Furthermore, because of significant technology limitations, there is

---

[29] U.S. Department of Homeland Security, *Department of Homeland Security Transportation Security Administration Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 47-49.

[30] "Aviation and Transportation Security Act" (P.L. 107-71 §110).

[31] See, for example, (a) GAO, *Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO-03-843,* (Washington: U.S. General Accounting Office, June 30, 2003), 23; (b) GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington: U.S. General Accounting Office, December 20, 2002); and report of the TSA Aviation Security Advisory Committee, October 1, 2003. http://www.tsa.gov/public/display?theme=44&content=090005198005906d.

[32] For fiscal year 2004, Congress provided funds for 100 TSA inspectors "to perform more in-depth audits of shipper compliance with the known shipper requirement." House Report 108-280 accompanying the Department of Homeland Security Appropriations Act of Fiscal Year 2004. The Administration's budget request for fiscal year 2005 includes the same funding level for inspection of known shipper compliance. U.S. Department of Homeland Security, *Department of Homeland Security Transportation Security Administration Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 47-49.

[33] GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington: U.S. General Accounting Office, December 20, 2002), 8.

[34] GAO, *Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO-03-843,* (Washington: U.S. General Accounting Office, June 30, 2003), 23.

[35] This exemption is significant as the explosive device used in Pan Am flight 103 is estimated to have weighed approximately 16 ounces. The explosive brought on board by Richard Reid is also estimated to have weighed less than one pound.

[36] U.S. Senate, Committee on Commerce, Science and Transportation, *Status of Aviation Security One Year After September 11* Hearing, September 10, 2002.

no practical way to achieve 100 percent manual screening/inspection of air cargo."[37] As a result of this claim, based on a study conducted before September 11, 2001, Congress did not enact legislation that would have required 100 percent screening of air cargo on passenger aircraft.[38] One reason given is that detection systems, such as the VACIS machine used to screen containers at seaports, are not sufficiently sensitive to identify the relatively small amounts of explosives needed to cause major damage to an aircraft.[39] Secretary Tom Ridge, however, has indicated that the technology exists to screen all cargo.[40]

Rather than screening all cargo, TSA has announced plans to screen all "high-risk" cargo in the future. However, TSA has little experience or expertise in determining risk and intends to benefit from the experience built by the Bureau of Customs and Border Protection (CBP).[41] Unfortunately, CBP's risk assessment process is problematic. According to GAO, "while CBP's strategy incorporates some elements of risk management, it does not include other key elements, such as a comprehensive set of criticality, vulnerability and risk assessments that experts told GAO are necessary to determine risk and the types of responses necessary to mitigate that risk. Also, CBP's targeting system does not include a number of recognized modeling practices, such as subjecting the system to peer review, testing and validation."[42]

SECURITY RECOMMENDATION

The TSA should provide adequate security for air cargo, with the ultimate goal of 100 percent inspection as soon as possible. The "known shipper" program should be strengthened by regularly verifying that that all participating companies are following all security procedures,

(Continued on following page)

[37] Letter from Asa Hutchinson, Under Secretary for Border and Transportation Security, to Senator Thad Cochran, July 8, 2003.

[38] The U.S. House of Representatives passed the Homeland Security Appropriations Act for Fiscal Year 2004 with an amendment requiring complete screening of cargo transported on passenger planes. The Senate, following the letter from Under Secretary Hutchinson to Senator Thad Cochran, Chairman of the Senate Appropriations Subcommittee on Homeland Security, did not include such a requirement. The enacted legislation required only that "The Secretary of Homeland Security is directed to research, develop, and procure certified systems to inspect and screen air cargo on passenger aircraft at the earliest date possible: *Provided*, that until such technology is procured and installed, the Secretary shall take all possible actions to enhance the known shipper program to prohibit high-risk cargo from being transported on passenger aircraft." "Department of Homeland Security Appropriations Act of Fiscal Year 2004" (P.L. 108-90 §521).

[39] Presentation to House Select Committee on Homeland Security staff by TSA, January 15, 2004.

[40] During the question period of a hearing of the House Select Committee on Homeland Security, Representative Ed Markey stated "…technology exists. The only question is, how much money are you willing to spend on it? The technology is there that can screen the cargo." Secretary Ridge responded, "That's exactly right." U.S. House, Select Committee on Homeland Security, *How is America Safer: A Progress Report on the Department of Homeland Security* Hearing, May 20, 2003

[41] TSA, "Air Cargo Strategic Plan," November 2003. http://www.tsa.gov/public/display?theme=44&content=0900051980069bfe.

[42] GAO, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers, GAO-04-325T*, (Washington: U.S. General Accounting Office, December 16, 2003), ii.

perhaps through third parties inspections.[43] The TSA should deploy similar detection equipment as is currently used for airline baggage,[44] U.S. mail, and large shipping containers to inspect cargo on passenger planes while continuing to develop better technology options. Where electronic screening is currently impossible, other detection methods, including canine screening and hand searches, should be used as an interim solution.

- **All-Cargo Aircraft**

In addition to securing cargo on passenger planes, all-cargo aircraft are also at risk of terrorist attack. These aircraft, which are as large as passenger planes, could be hijacked and used as missiles. For this reason, TSA has limited passengers on these planes to those necessary for the flight and delivery of cargo, and requires that cargo planes either have hardened cockpit doors or meet alternate security measures.[45] However, all-cargo aircraft that overfly the United States without landing are not subject to these security measures. This loophole is especially significant as DHS has cited intelligence that terrorists are seeking weaknesses in international flights.[46]

SECURITY RECOMMENDATION

TSA should extend security measures, including hardening cockpit doors and limiting non-essential passengers, to all cargo aircraft that overfly the United States.

SECURITY GAP: Passenger Aircraft are Vulnerable to Missile Attack.

The threat to commercial aviation from shoulder-fired missiles is immediate and severe. Terrorists have demonstrated an interest in using such "man portable air defense systems" (MANPADS),[47] have possession or access to them, and face no significant defense against the proven efficacy of missile attack. For example, on August 12, 2003, Hemant Lakhani was arrested in Newark, New Jersey, after trying to sell a shoulder-fired missile to a Federal Bureau of Investigation (FBI) operative posing as an extremist who wanted to shoot down a commercial airplane. On November 28, 2002, terrorists fired two SA-7 MANPADS at an Israeli charter jet departing Mombasa, Kenya. Terrorists with links to al Qaeda were recently arrested in Hong Kong when attempting to purchase MANPADS from undercover FBI agents.[48] The use of shoulder-fired missiles is widespread in attacks against military aircraft – it has been estimated

[43] "According to TSA officials, in 1999 FAA requested funds to conduct a feasibility study on a system of third-party inspections, but the study was not funded by the Congress." GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington: U.S. General Accounting Office, December 20, 2002), 9.

[44] As recommended by the Gore Commission and the Cargo Working Group. See GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington: U.S. General Accounting Office, December 20, 2002), 12.

[45] See 14 CFR - CHAPTER I - PART 129 §129.28 Flightdeck security. Some cargo planes do not have cabins that would allow a cockpit door, and are instead required to meet TSA-approved alternate security measures.

[46] Statement of Secretary Tom Ridge upon raising of the terrorist threat level, December 21, 2003.

[47] MANPADS also include classes of shoulder-fired missiles (SAMs).

[48] See, for example, Ralph Vartabedian, "U.S. Officials Announce 2 Terrorism Indictments," *Los Angeles Times*, November 7, 2002, 5.

that man-portable missiles caused 90 percent of worldwide combat aircraft losses from 1984-2001,[49] and they have been used against aircraft using Baghdad International Airport during and after Operation Iraqi Freedom in Iraq.

Estimates of the global inventory of man portable missiles range from 250,000 to 700,000 systems, and they are available at reasonably low cost.[50] Some estimate that 27 militia groups and terrorist organizations possess such weapons.[51]

Due to the widespread availability and small size of shoulder-fired missiles, there can be no guarantee that they will be kept out of the United States or away from foreign destinations of U.S. air carriers. Due to the missiles' reasonably long range, they can be fired at airplanes from substantial distances away from airports, making airport perimeter security alone an insufficient defense.

The DHS has begun a two year, $121 million program to investigate countermeasure technologies for missile attacks.[52] The Science and Technology Directorate has established a Counter-MANPADs Special Program Office for this purpose and plans to investigate both adapting existing technologies from military aircraft defense systems and developing new technologies.

SECURITY RECOMMENDATION

The DHS should continue this research and development effort and should prepare plans for deploying missile countermeasure technologies onto passenger airplanes. Such plans should include options for deploying defenses on aircraft under heightened risk of attack, either because of the size of airplane or regular flight routes.

Additional steps should also be taken beyond missile countermeasures. Inspectors at TSA and Customs and Border Protection (CBP) should incorporate specific training for screeners and border inspectors to identify the missiles, and these agencies should work with counterparts overseas to do the same. State and local governments and law enforcement should be given additional guidance to help identify locations at high risk for missile firings, based on flight paths and location accessibility. Finally, the Administration should push to duplicate globally the

(Continued on following page)

[49] Michael Puttre, "Facing the Shoulder-Fired Threat," *Journal of Electronic Defense,* April 1, 2001, No. 4, Vol. 24, 38.

[50] According to the Congressional Research Service "The missiles are about 5 to 6 feet in length, weigh about 35 to 40 pounds, and, depending on the model, can be purchased on the black market anywhere from a few hundred dollars for older models to upwards of almost a quarter million dollars for newer, more capable models. Shoulder-fired SAMs generally have a target detection range of about 6 miles and an engagement range of about 4 miles…. Published estimates on the number of missiles presently being held in international military arsenals range from 350,000 to 500,000…, estimates of shoulder-fired SAMs in terrorist hands vary considerably. Estimates range from 5,000 to 150,000 of various missile types." Congressional Research Service, *Homeland Security: Protecting Airliners from Terrorist Missiles, RL31741*, (Washington: Congressional Research Service, November 3, 2003), 1, 3, 4.

[51] Vivienne Walt, "Portable Missiles Concern Senators," *USA Today*, December 2, 2002, 1.

[52] This includes $60 million appropriated for fiscal year 2004 and $61 million included in the President's request for fiscal year 2005.

recent agreement of the Asia Pacific Economic Group to "adopt strict domestic export controls on MANPADs; secure stockpiles; regulate MANPADs production, transfer, and brokering; ban transfers to non-state end users; and exchange information in support of these efforts."[53]

SECURITY GAP: Unscreened Airport Employees and Vendors Can Gain Access to Secure Parts of Airports.

Congress has required that airport perimeters be secure, including the "screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States…" that will "assure at least the same level of protection as will result from screening of passengers and their baggage."[54] Yet, while TSA has spent billions of dollars to screen all passengers and flight crews traveling on U.S. passenger planes, it is TSA policy that airport workers may access sensitive locations without such checks.[55] Thousands of vendor employees that work in airport terminals can bypass security screening once they have gone through a rudimentary background check and could potentially board an aircraft or give prohibited items to a passenger.

A similar security loophole exists for the workers that service the airplanes for food service, cleaning and maintenance, and loading cargo. The potential for harm in this system was demonstrated recently when 25 people, mostly current or former employees at John F. Kennedy Airport in New York were arrested for participating in a complex and long-running drug smuggling operation.[56]

Even more troubling, previous investigations have shown that unauthorized persons have been able to access airports and airplanes with false identification. The DHS Office of the Inspector General conducted testing in which unauthorized personnel were able "to gain access to the security checkpoints and consequently the sterile area of most of the airports tested."[57] In addition, TSA has found that hundreds of its own employees used false information on applications and job materials that allowed them to gain access to sensitive airport locations.[58] Gaps in security at airport perimeters have also been documented. In one recent media account, journalists were able to gain access to the tarmac at large airports and could have reached passenger planes on the ground.[59]

---

[53] (a) The White House, "Fact Sheet: New APEC Initiatives on Counterterrorism," October 21, 2003. http://www.whitehouse.gov/news/releases/2003/10/20031021-4.html; (b) Philip Shenon, "U.S. Reaches Deal to Limit Transfers of Portable Missiles," *The New York Times*, October 21, 2003, A1.

[54] "Aviation and Transportation Security Act" (P.L. 107-71 §106).

[55] U.S. House, Committee on Homeland Security, *Identification Documents Fraud and the Implications for Homeland Security* Hearing, October 1, 2003

[56] Robert F. Worth, "20 Airport Workers Held in Smuggling Of Drugs for Decade," *The New York Times*, A1.

[57] Department of Homeland Security, Office of Inspector General, "Fiscal Year 2004 Annual Performance Plan," 23. http://www.dhs.gov/interweb/assetlibrary/FY2004_Performance_Plan.pdf.

[58] GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs, GAO-04-285T*, (Washington: U.S. General Accounting Office, November 20, 2003), 18.

[59] Steve McVicker, "Local airports may have security flaws; Expert decries 'easy access'," *Houston Chronicle*, January 7, 2004, A1.

SECURITY RECOMMENDATION

The TSA should adopt policies to ensure that everyone with the potential to harm passenger airplanes is appropriately screened. Everyone and everything that reaches a part of the airport physically beyond the screening checkpoints should be required to undergo inspection. Similarly, anyone seeking to gain access to a sensitive or secure airport location should be required to present tamper-proof, biometric identification. Airport perimeters should also be made more secure, using a combination of physical defenses, surveillance, and patrols. The TSA should meet all of the requirements set in law for airport perimeter security.[60]

[60] GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs, GAO-04-285T*, (Washington: U.S. General Accounting Office, November 20, 2003), 18-19.